Understanding the Cloud Components, Security Issues, and Emerging Solutions that Potentially Mitigate the Vulnerabilities in Networks

Veenababu Kannika Sherly

Research Analyst, SMRVD Security Solutions, India.

Abstract

The objective of this research is to understand the cloud components, security issues, and dangers, along with emerging solutions that may potentially mitigate the vulnerabilities in the cloud. It is a commonly accepted fact that, cloud is a viable hosting platform; however, the perception with respect to security in the cloud is that it needs significant improvements to realize higher rates of adaption in the enterprise scale. As identified by another research, many of the issues confronting the cloud computing need to be resolved urgently.

Keywords: Cloud computing; Security Threats; Privacy.

1. Introduction

With so much of our workload moving to cloud, security in cloud computing is under increased scrutiny. This assessment is also supported by the 2017 report by Forbes, which says that in 15 months, while 80% of all IT budgets will be committed to cloud solution, 49% of the businesses are delaying cloud deployment due to security skills gap and concerns. The problem appears to be multi-dimensional, with lack of skilled resources, lack of maturity, conflicting best practices, and complex commercial structures to name a few.

Cloud Storage as a service is a growing trend with features like elasticity, pay-as-you-go, business 12 continuity with long-term retention and risk mitigation through disaster recovery. All these features 13 are not available with on-premises storage. Popular cloud-based storage services available today are Dropbox, One Drive, Amazon S3, Google Drive, Box, and Sugar Sync etc. Nowadays, to improve business strategies organizations use analysis techniques over their historical data. Some business sectors for instance telecom and e-health have compliance requirements, which bind them to keep historical data over a specified period. Not every organization is equipped to manage large secondary storage or build their private data centers (because of the cost associated with building and maintaining such infrastructure). Cloud Storage can be of great service to such organizations because of its flexible model [1-11]. However, the loss of control is an inherent issue with outsourced data storage model.

Although the cloud service provider (CSP) is bounded by a service level agreement (SLA) to ensure data security, users cannot solely rely on such agreements. Furthermore, reliance on a contractual obligation may fail to detect the malicious behavior of the service provider. Cloud computing operational details are not transparent to the customers and the CSP may be untrusted [12-23]. So besides the convenience provided by cloud model, data security issues such as confidentiality, privacy, and data integrity are also associated with cloud storage service model. Data can be manipulated or lost due to accidental or intentional malicious activity, which can be a nightmare for the user and an embarrassment for cloud service provider. Cloud has a provision of “multi-tenancy” i.e. cloud resources will be shared and utilized by multiple users; therefore, adversaries can take advantage of vulnerabilities in the cloud.

Adaption of cloud has reached a tipping point and it is expected that more workloads will move from traditional local storage to cloud from not just average Internet users, but also from most if not all commercial entities. While there are many problems that need identifying, analyzing, and addressing, this document attempts to survey the security in cloud computing and reports on various aspects of security vulnerabilities and solutions [24-39]. Some questions that need urgent answers are: (a) Privileged User Access Management, (b) Regulatory Compliance, (c) Data Location, (d) Data Segregation, (e) Data Protection and Recovery Support, (f) Investigative Support, and (g) Long-term Viability.

It is highly recommended that these questions, along with other risks, are assessed and addressed. Some of the assessments could be as follows:

1. Organization capability and maturity
2. Technology & data risks
3. Application migration and performance risk
4. People risks
5. Process risks

This article consolidates various works that address the risks, vulnerabilities, and potential controls in cloud computing. It also provides information on leading cloud architectures and frameworks. Moreover, the article identifies potential future research areas related to security in cloud computing. Before we dive into the security issues [40-50], it is important to understand the cloud definition and architecture. Cloud computing is a set of resources that can scale up and down on-demand. It is available over the Internet in a self-service model with little to no interaction required with the service provider. Cloud enables new ways of offering products and services with innovative, technical, and pricing opportunities.

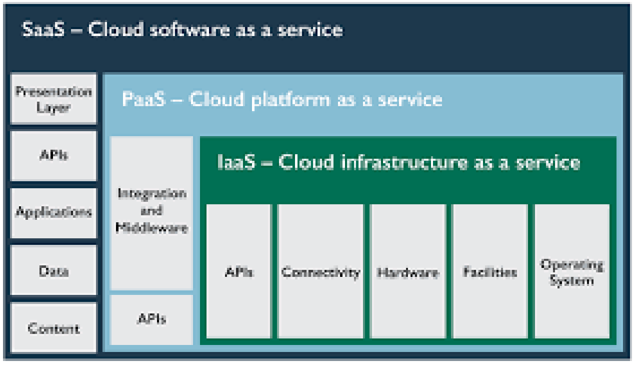
SaaS – Cloud software as a service
Presentation Layer
APIs
Applications
Data
Content
PaaS – Cloud platform as a service
Integration and Middleware
APIs
IaaS – Cloud infrastructure as a service
APIs
Connectivity
Hardware
Facilities
Operating System

Figure 1. Cloud Computing Architecture (Source: Internet)

As per NIST’s Cloud Computing Reference Architecture, there are five major factors that influence and are impacted by cloud computing, along with its security implications. This document focuses on cloud consumer and cloud provider’s threat and risk perceptions. It is important to note that the this represents an end-to- end reference architecture that addresses all the seven layers of the Open Systems Interconnection (OSI) model, and extends to include the business, commercial, and governance aspects. As it is evident, cloud computing is a comprehensive and complex solution with many areas of vulnerabilities.

2. Deployment and Delivery Models

The two most important aspects that determine the level of vulnerability in a cloud-computing platform is the choice of deployment and delivery model. There are three deployment and three delivery models that are considered as industry standards. Each of these three deployment and delivery models have unique security implications. The following sub-sections briefly discuss each of these models and their security implications:

The three most common types of cloud deployment models are Private Cloud, Public Cloud, and Hybrid Cloud. The three cloud delivery models proposed by NIST and adapted by the industry are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Cloud computing, like other areas of IT, suffers from a number of security issues, which need to be addressed. These risks pertain to policy and organization risks, technical risks, and legal and other risks.

Cloud is a set of technology, process, people, and commercial construct. Like all other technology, process, people, and commercial construct, cloud too has vulnerabilities. The following are some of the vulnerabilities in a cloud. Some of the open issues and threats that needs urgent attention are as follows:

Shared Technology vulnerabilities – increased leverage of resources gives the attackers a single point of attack, which can cause damage disproportional to its importance. An example of share technology is a hypervisor or cloud orchestration. Data Breach – with data protection moving from cloud consumer to cloud service provider, the risk of accidental, malicious, and intentional data breach is high. Account of Service traffic hijacking – one of the biggest advantages of cloud is access through Internet, but the same is a risk of account compromise. Loosing access to privileged account might mean loss of service. Denial of Service (DoS) – any denial of service attack on the cloud provider can affect all tenets.

Malicious Insider – a determined insider can find more ways to attack and cover the track in a cloud scenario. Internet Protocol – many vulnerabilities inherent in IP such as IP spoofing, ARP spoofing, DNS Poisoning are real threats. Injection Vulnerabilities – vulnerabilities such as SQL injection flaw, OS injection, and LDAP injection at the management layer can cause major issues across multiple cloud consumers. API & Browser Vulnerabilities – Any vulnerability in cloud provider’s API or Interface poses a significant risk, when coupled with social engineering or browser based attacks; the damage can be significant.

Changes to Business Model – cloud computing can be a significant change to a cloud consumer’s business model. IT department, and business needs to adapt or face exposure to risk. Abusive use – certain features of cloud computing can be used for malicious attack purposes such as the use of trail period of use to launch zombie or DDoS attacks. Malicious Insider – a malicious insider is always a major risk, however, a malicious insider at the cloud provider can cause significant damage to multiple consumers. Availability –the probability that a system will work as required and when required.

According to a recent research, the three major vectors of attack are network, hypervisor, and hardware. These vectors are mapped to attacks such as external, internal, and cloud provider or insider attack respectively.

The vulnerabilities and threats in the cloud are well documented. Each cloud service provider and cloud consumer has to devise countermeasures and controls to mitigate the risks based on their assessment. However, the following are some of the best practices in countermeasures and controls that can be considered: End-to-end encryption – the data in a cloud delivery model might traverse through many geographical locations; it is imperative to encrypt the data end-to-end. Scanning for malicious activities – end-to-end encryption while highly recommended, induces new risks, as encrypted data cannot be read by the Firewall or IDS. Therefore, it is important to have appropriate controls and countermeasures to mitigate risks from malicious software passing through encryption.

Validation of cloud consumer – the cloud provider has to take adequate precautions to screen the cloud consumer to prevent important features of cloud being used for malicious attack purposes. Secure Interfaces and APIs – the interfaces and APIs are important to implement automation, orchestration, and management. The cloud provider has to ensure that any vulnerability is mitigated. Insider attacks – cloud providers should take precaution to screening employee and contractors, along with strengthening internal security systems to prevent any insider attacks. Secure leveraged resources – in a shared/multi-tenancy model, the cloud provider has secure shared resources such as hypervisor, orchestration, and monitoring tools. Business Continuity plans – Business continuity plan is a process of documenting the response of the organization to any incidents that cause unavailability of whole or part of a business-critical process.

3. Conclusions

The vulnerabilities and threats in the cloud are well documented. Each cloud service provider and cloud consumer has to devise countermeasures and controls to mitigate the risks based on their assessment. It is important to take this research forward to provide such best practices to more applications and use cases. It is also essential to conduct further research in systems development life cycle (SDLC) for cloud consumers to incorporate various development and technological advancement models and container systems such as Docker to improve security at a fundamental level. Additionally, there is very limited research on training and people impact on security. Work can be done to understand the challenges, requirements, and impact of effective security training for consumers and other providers.

References

[1] Yu, Y.; Ni, J.; Au, M. H.; Liu, H.; Wang, H. & Xu, C. (2014), 'Improved security of a dynamic remote data possession checking protocol for cloud storage', Expert Syst. Appl. 41(17), 7789-7796.

[2] 'MuR-DPA: Top-down Levelled Multi-replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud', Computers, IEEE Transactions on PP(99), 1-1.

[3] Miao, M.; Jiang, T. & You, I. (2015), 'Payment-based incentive mechanism for secure cloud deduplication ', International Journal of Information Management.

[4] Latesh Kumar, K. & Lawrance, R. (2015), Novel Approach: Deduplication for Backup Systems Using Data Block Size, in Lakhmi C. Jain; Himansu Sekhar Behera; Jyotsna Kumar Mandal & Durga Prasad Mohapatra, ed., 'Computational Intelligence in Data Mining - Volume 1', Springer India, , pp. 365-373.

[5] Vinod Varma Vegesna (2017). “Incorporating Wireless Sensor Networks and the Internet of Things: A Hierarchical and Security-Based Analysis,” International Journal of Current Engineering and Scientific Research, Volume-4, Issue-5, Pages 94-106, Available at SSRN: https://ssrn.com/abstract=4418110

[6] Vinod Varma Vegesna (2016). “Threat and Risk Assessment Techniques and Mitigation Approaches for Enhancing Security in Automotive Domain,” International Journal of Management, Technology And Engineering, Volume VI, Issue II, July-Dec 2016, Pages 314-331, Available at SSRN: https://ssrn.com/abstract=4418100

[7] Hamid Ali Abed Al-Asadi, et al., “Nature Inspired Algorithms multi-objective histogram equalization for Grey image enhancement”, Advances in Computer, Signals and Systems (2020) 4: 36-46 Clausius Scientific Press, Canada DOI: 10.23977/acss.2020.040106.

[8] Hamid Ali Abed Al-Asadi and et al., “ Critical Comparative Review of Nature-Inspired Optimization Algorithms (NIOAs), International Journal of Simulation: Systems, Science and Technology (IJSSST), 2020, 21(3), PP1-15

[9] Hamid Ali Abed Al-Asadi, (2022) “1st Edition: Privacy and Security Challenges in Cloud Computing A Holistic Approach" Intelligent Internet of Things for Smart Healthcare Systems, Scopus, Taylor @Francis, CRC Press. (Book Chapter: Enhanced Hybrid and Highly Secure Cryptosystem for Mitigating Security Issues in Cloud Environments), March 2022.

[10] Vinod Varma Vegesna (2015). “Incorporating Data Mining Approaches and Knowledge Discovery Process to Cloud Computing for Maximizing Security,” International Journal of Current Engineering and Scientific Research, Volume-2, Issue-6, Pages 118-133, Available at SSRN: https://ssrn.com/abstract=4418107

[11] Wei, L.; Zhu, H.; Cao, Z.; Dong, X.; Jia, W.; Chen, Y. & Vasilakos, A. V. (2014), Security and Privacy for 23 Storage and Computation in Cloud Computing, Inf. Sci. 258, 371-386.

[12] Wang, H. & Zhang, Y. (2014), On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multicloud Storage, Parallel and Distributed Systems, IEEE Transactions on 25(1), 264-267.

[13] Yu, Y.; Ni, J.; Ren, J.; Wu, W.; Chen, L. & Xia, Q. (2014), Improvement of a Remote Data Possession Checking Protocol from Algebraic Signatures, in Xinyi Huang & Jianying Zhou, ed., 'Information Security Practice and Experience', Springer International Publishing, pp. 359-372.

[14] Chen, L.; Guo, G. & Peng, Z. (2014), 'A hill cipher-based remote data possession checking in cloud storage', Security and Communication Networks 7(3), 511-518.

[15] Vinod Varma Vegesna (2021). “The Applicability of Various Cyber Security Services for the Prevention of Attacks on Smart Homes,” International Journal of Current Engineering and Scientific Research, Volume-8, Issue-12, Pages 14-21.

[16] Vinod Varma Vegesna (2020). “Secure and Privacy-Based Data Sharing Approaches in Cloud Computing for Healthcare Applications,” Mediterranean Journal of Basic and Applied Sciences, Volume 4, Issue 4, Pages 194-209, October-December 2020, doi: 10.46382/mjbas.2020.4409.

[17] Hamid Ali Abed Al-Asadi and et al., “Priority Incorporated Zone Based Distributed Clustering Algorithm For Heterogeneous Wireless Sensor Network”, Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 5, PP. 306-313, 2019.

[18] Hamid Ali Abed Al-Asadi and et al., “A Network Analysis for Finding the Shortest Path in Hospital Information System with GIS and GPS, Journal of Network Computing and Applications (2020) 5: 10-22.

[19] Vinod Varma Vegesna (2019). “Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes”, Indo-Iranian Journal of Scientific Research, Volume 3, Issue 1, Pages 69-84, January-March 2019, Available at SSRN: https://ssrn.com/abstract=4418119

[20] Vinod Varma Vegesna (2018). “Analysis of Artificial Intelligence Techniques for Network Intrusion Detection and Intrusion Prevention for Enhanced User Privacy”, Asian Journal of Applied Science and Technology, Volume 2, Issue 4, Pages 315-330, Oct-Dec 201.

[21] González-Manzano, L. & Orfila, A. (2015), 'An efficient confidentiality-preserving Proof of Ownership for deduplication', Journal of Network and Computer Applications 50(0), 49-59.

[22] Xiong, J.; Yao, Z.; Ma, J.; Liu, X. & Li, Q. (2013), A Secure Document Self-Destruction Scheme: An ABE Approach, in 'High Performance Computing and Communications 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference', pp. 59-64.

[23] Vinod Varma Vegesna (2021). “Analysis of Data Confidentiality Methods in Cloud Computing for Attaining Enhanced Security in Cloud Storage,” Middle East Journal of Applied Science & Technology, Vol. 4, Iss. 2, Pages 163-178, April-June 2021, Available at SSRN: https://ssrn.com/abstract=4418127

[24] Hamzah F. Zmezm, Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, "A Novel Scan2Pass Architecture for Enhancing Security towards E-Commerce," Future Technologies Conference 2017, 29-30 November 2017 | Vancouver, BC, Canada, 2017.

[25] Hamid Ali Abed Al-Asadi, Majida Ali Al-Asadi, Nada Ali Noori , "Optimization Noise Figure of Fiber Raman Amplifier based on Bat Algorithm in Optical Communication network," International Journal of Engineering & Technology, Scopus, Vol 7, No 2, pp. 874-879, 2018.

[26] Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, Hamzah F. Zmezm, Dr. Hussain Falih Mahdi, Hassan Muhsen Abdulkareem Al-Haidari. "Suggested Mechanisms for Understanding the Ideas in Authentication System," International Journal of Advancements in Computing Technology9(3):10-24, 2018.

[27] Vinod Varma Vegesna (2021). “A Highly Efficient and Secure Procedure for Protecting Privacy in Cloud Data Storage Environments,” International Journal of Management, Technology and Engineering, Volume XI, Issue VII, July 2021, Pages 277-287.

[28] Vinod Varma Vegesna (2021). “The Utilization of Information Systems for Supply Chain Management for Multicomponent Productivity Based on Cloud Computing,” International Journal of Management, Technology and Engineering, Volume XI, Issue IX, September 2021, Pages 98-113.

[29] Tang, Y.; Lee, P.; Lui, J. & Perlman, R. (2012), 'Secure Overlay Cloud Storage with Access Control and Assured Deletion', Dependable and Secure Computing, IEEE Transactions on 9(6), 903-916.

[30] Deswarte, Y.; Quisquater, J.-J. & Saïdane, A. (2004), Remote Integrity Checking, in Sushil Jajodia & Leon Strous, ed., 'Integrity and Internal Control in Information Systems VI', Springer US, pp. 1-11.

[31] Gazzoni, E. L.; Luiz, D.; Filho, G.; Sérgio, P.; Barreto, L. M. & Politécnica, E. (2006), 'Demonstrating Data Possession and Uncheatable Data Transfer'.

[32] Han, S.; Liu, S.; Chen, K. & Gu, D. (2014), Proofs of Retrievability Based on MRD Codes, in Xinyi Huang & Jianying Zhou, ed., 'Information Security Practice and Experience', Springer International Publishing, , pp.38 330-345.

[33] Cachin, C.; Haralambiev, K.; Hsiao, H.-C. & Sorniotti, A. (2013), Policy-based Secure Deletion, in 'Proceedings of the 2013 ACM SIGSAC Conference on Compute & Communications Security', ACM, New York, NY, USA, pp. 259-270.

[34] Vinod Varma Vegesna (2022). “Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks,” International Journal of Management, Technology and Engineering, Volume XII, Issue VII, July 2022, Pages 81-94.

[35] Hamid Ali Abed Al-Asadi, Majida Ali Abed, AL-Asadi, Zainab sabah, Baha Al-Deen, Ahmad Naser Ismail, “Fuzzy Logic approach to Recognition of Isolated Arabic Characters”, International Journal of Computer Theory and Engineering, Vol. 2, No. 1, 1793-8201, February, 2010.

[36] H. A. Al-Asadi, M.H. Al-Mansoori, S. Hitam, M. I. Saripan, and M. A. Mahdi, “Particle swarm optimization on threshold exponential gain of stimulated Brillouin scattering in single mode fibers,” Optics Express, vol. 19, no. 3, pp. 1842-1853, 2011.

[37] Majida Al-Asadi, Yousif A. Al-Asadi, Hamid Ali Abed Al-Asadi, "Architectural Analysis of Multi-Agents Educational Model in Web-Learning Environments," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 6, 2012.

[38] Vinod Varma Vegesna (2022). “Accelerate the development of a business without losing privacy with the help of API Security Best Practises - Enabling

businesses to create more dynamic applications," International Journal of Management, Technology and Engineering, Volume XII, Issue IX, September 2022, Pages 91-99.

[39] Chaoling, L.; Yue, C. & Yanzhou, Z. (2014), 'A data assured deletion scheme in cloud storage', Communications, China 11(4), 98-110.

[40] Bellare, M.; Keelveedhi, S. & Ristenpart, T. (2013), DupLESS: Server-aided Encryption for Deduplicated Storage, in 'Proceedings of the 22Nd USENIX Conference on Security', USENIX Association, Berkeley, CA, USA, pp. 179-194.

[41] Vinod Varma Vegesna (2022). "Using Distributed Ledger Based Blockchain Technological Advances to Address IoT Safety and Confidentiality Issues," International Journal of Current Engineering and Scientific Research, Volume-9, Issue-3, Pages 89-98.

[42] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "Simplifying Handwritten Characters Recognition Using a Particle Swarm Optimization Approach", European Academic Research, Vol 1,pp. 535- 552, Issue(5), 5. 2013.

[43] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "High Accuracy Arabic Handwritten Characters Recognition using (EBPANN) Architecture," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6 Issue 2, 2015.

[44] Hamid Ali Abed Al-Asadi and Majda Ali Abed, "Object Recognition Using Artificial Fish Swarm Algorithm on Fourier Descriptors," American Journal of Engineering, Technology and Society; Volume 2, Issue 5: pp. 105-110, 2015.

[45] Vinod Varma Vegesna (2022). "Methodologies for Enhancing Data Integrity and Security in Distributed Cloud Computing with Techniques to Implement Security Solutions," Asian Journal of Applied Science and Technology, Volume 6, Issue 2, Pages 167-180, April-June 2022, doi: 10.38177/ajast.2022.6217.

[46] Ohmin Kwon, Dongyoung Koo, Yongjoo Shin, and Hyunsoo Yoon, "A Secure and Efficient Audit Mechanism for Dynamic Shared Data in Cloud Storage," The Scientific World Journal, vol. 2014, Article ID 820391, 10 pages, 2014.

[47] Harnik, D.; Pinkas, B. & Shulman-Peleg, A. (2010), 'Side Channels in Cloud Services: Deduplication in Cloud Storage', IEEE Security & Privacy 8(6), 40-47.

[48] Rahumed, A.; Chen, H.; Tang, Y.; Lee, P. & Lui, J. (2011), A Secure Cloud Backup System with Assured Deletion and Version Control, in 'Parallel Processing Workshops (ICPPW), 2011 40th International Conference, pp. 160-167.

[49] Tang, Y.; Lee, P.; Lui, J. & Perlman, R. (2012), 'Secure Overlay Cloud Storage with Access Control and Assured Deletion', Dependable and Secure Computing, IEEE Transactions 9(6), 903-916.

[50] Reardon, J.; Basin, D. & Capkun, S. (2013), SoK: Secure Data Deletion, in 'Security and Privacy (SP), 2013 IEEE Symposium', pp. 301-315.